

**AMENDMENTS TO THE CLAIMS**

1     1.     (Previously Presented) A method for managing addition and deletion of network nodes  
2             from and to a secure multicast or broadcast group of network nodes in a communications  
3             network without a single point of failure, wherein each of the network nodes is associated  
4             with one of a plurality of group controllers, wherein each group controller of the plurality  
5             of group controllers is a replica of a particular group controller, and wherein the network  
6             nodes and the plurality of group controllers are logically organized in a binary tree that  
7             represents the network nodes and the plurality of group controllers, in which leaf nodes  
8             of the binary tree represent network nodes that are joining or leaving the secure multicast  
9             or broadcast group, intermediate nodes represent other network nodes, and root nodes  
10            represent the plurality of group controllers, the method comprising the steps of:  
11            joining a first group controller to the plurality of group controllers in a local network;  
12            establishing a secure communication channel between the first group controller and a  
13                second group controller of the plurality of group controllers using a key exchange  
14                protocol;  
15            receiving a request to add or delete a network node of the secure multicast or broadcast  
16                group from a load balancer that is coupled to the plurality of group controllers;  
17            creating and storing a new group session key for each network node represented in each  
18                branch of the binary tree that is affected by adding or deleting the network node  
19                from the secure multicast or broadcast group; and  
20            distributing a group session key from a third group controller of the plurality of group  
21                controllers to the network nodes.

1     2.     (Previously Presented) A method as recited in Claim 1, wherein distributing a group  
2             session key further comprises:  
3             receiving a token value at the third group controller to designate the third group controller  
4                as having permission to selectively generate the group session key and to generate  
5                node keys associated with the intermediate nodes and the leaf nodes; and  
6             creating and storing the group session key only when the third group controller has the  
7                token value.

- 1 3. (Previously Presented) A method as recited in Claim 1, wherein distributing a group  
2 session key further comprises:  
3 determining whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected by the leaving node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key; and  
8 sending the new group session key to the leaf nodes.
- 1 4. (Previously Presented) A method as recited in Claim 3, wherein updating keys  
2 comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.
- 1 5. (Previously Presented) A method as recited in Claim 1, wherein distributing a group  
2 session key further comprises:  
3 receiving a request message from one of the network nodes to join the secure multicast or  
4 broadcast group;  
5 determining which of the intermediate nodes are affected by the joining node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key and a private key of the joining node; and  
8 sending a message comprising the new group session key, the private key, and the  
9 updated keys of affected intermediate nodes to the joining node.
- 1 6. (Original) A method as recited in Claim 5, wherein updating keys comprises performing  
2 a one way hash function on the keys associated with the affected intermediate nodes.
- 1 7. (Original) A method as recited in Claim 1, wherein receiving a request comprises  
2 receiving the request at a load balancer having a single virtual address that represents the  
3 plurality of group controllers.

1 8. (Previously Presented) A method as recited in Claim 7, further comprising the step of  
2 load balancing network traffic that is directed from a plurality of the network nodes to the  
3 plurality of group controllers.

1 9. (Previously Presented) A method as recited in Claim 1, wherein establishing a secure  
2 communication channel comprises exchanging a public key of the first group controller  
3 with all other group controllers in the plurality of group controllers based upon optimized  
4 broadcast Diffie-Hellman protocol.

1 10. (Previously Presented) A method as recited in Claim 5, wherein establishing a secure  
2 communication channel comprises:  
3 receiving a public key value that is broadcast by the joining node;  
4 sending a collective public key value from the network nodes to the joining node;  
5 computing a shared secret key; and  
6 creating and storing a group shared secret key by exchanging private key values.

1 11. (Currently Amended) A computer-readable storage medium comprising one or more  
2 sequences of executable instructions for managing addition and deletion of network  
3 nodes from and to a secure multicast or broadcast group of network nodes in a  
4 communications network without a single point of failure, wherein each of the network  
5 nodes is associated with one of a plurality of group controllers, wherein each group  
6 controller of the plurality of group controllers is a replica of a particular group controller,  
7 and wherein the network nodes and the plurality of group controllers are logically  
8 organized in a binary tree that represents the network nodes and the plurality of group  
9 controllers, in which leaf nodes of the binary tree represent network nodes that are  
10 joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
11 other network nodes, and root nodes represent the plurality of group controllers, and  
12 which instructions, when executed by one or more processors, cause the processors to  
13 carry out the steps of:  
14 joining a first group controller to the plurality of group controllers in a local network;

15 establishing a secure communication channel between the first group controller and a  
16 second group controller of the plurality of group controllers using a public key  
17 exchange protocol;  
18 receiving a request to add or delete a network node of the secure multicast or broadcast  
19 group from a load balancer that is coupled to the plurality of group controllers;  
20 creating and storing a new group session key for each network node represented in each  
21 branch of the binary tree that is affected by adding or deleting the network node  
22 from the secure multicast or broadcast group; and  
23 distributing a group session key from a third group controller of the plurality of group  
24 controllers to the network nodes.

1 12. (Currently Amended) A computer-readable storage medium as recited in Claim 11,  
2 wherein distributing a group session key further comprises:  
3 receiving a token value at the third group controller to designate the third group controller  
4 as having permission to selectively generate the group session key and to generate  
5 node keys associated with the intermediate nodes and the leaf nodes; and  
6 creating and storing the group session key only when the third group controller has the  
7 token value.

1 13. (Currently Amended) A computer-readable storage medium as recited in Claim 11,  
2 wherein distributing a group session key further comprises:  
3 determining whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected by the leaving node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key; and  
8 sending the new group session key to the leaf nodes.

- 1 14. (Currently Amended) A computer-readable storage medium as recited in Claim 3,  
2 wherein updating keys comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.
- 1 15. (Currently Amended) A computer-readable storage medium as recited in Claim 11,  
2 wherein distributing a group session key further comprises:  
3 receiving a request message from one of the network nodes to join the secure multicast or  
4 broadcast group;  
5 determining which of the intermediate nodes are affected by the joining node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key and a private key of the joining node; and  
8 sending a message comprising the new group session key, the private key, and the  
9 updated keys of affected intermediate nodes to the joining node.
- 1 16. (Currently Amended) A computer-readable storage medium as recited in Claim 15,  
2 wherein updating keys comprises performing a one way hash function on the keys  
3 associated with the affected intermediate nodes.
- 1 17. (Currently Amended) A computer-readable storage medium as recited in Claim 11,  
2 wherein receiving a request comprises receiving the request at a load balancer having a  
3 single virtual address that represents the plurality of group controllers.
- 1 18. (Currently Amended) A computer-readable storage medium as recited in Claim 17,  
2 further comprising executable instructions which, when executed by the one or more  
3 processors, cause the processors to carry out the step of load balancing network traffic  
4 that is directed from a plurality of the network nodes to the plurality of group controllers.

1 19. (Currently Amended) A computer-readable storage medium as recited in Claim 11,  
2 wherein establishing a secure communication channel comprises exchanging a public key  
3 of the first group controller with all other group controllers in the plurality of group  
4 controllers based upon Diffie-Hellman protocol.

1 20. (Currently Amended) A computer-readable storage medium as recited in Claim 15,  
2 wherein establishing a secure communication channel comprises:  
3 receiving a public key value that is broadcast by the joining node;  
4 sending a collective public key value from the network nodes to the joining node;  
5 computing a shared secret key; and  
6 creating and storing a group shared secret key by exchanging private key values.

1 21. (Previously Presented) A method of managing addition and deletion of network nodes  
2 from and to a secure multicast or broadcast group of network nodes in a communications  
3 network, wherein each of the network nodes is associated with a first group controller  
4 comprising information that is replicated in a plurality of group controllers, and wherein  
5 the network nodes and the plurality of group controllers are logically organized in a  
6 binary tree that represents the network nodes and the plurality of group controllers, in  
7 which leaf nodes of the binary tree represent network nodes that are joining or leaving the  
8 secure multicast or broadcast group, intermediate nodes represent other network nodes,  
9 and root nodes represent the plurality of group controllers, the method comprising the  
10 steps of:  
11 joining the first group controller in a local network in which the plurality of group  
12 controllers are coupled;  
13 establishing a secure channel between the first group controller and the plurality of group  
14 controllers through secure key exchange;  
15 receiving a request to add or delete a network node from a load balancer that controls  
16 distribution of requests to the plurality of group controllers;  
17 generating a new group session key for each network node represented in each branch of  
18 the binary tree that is affected by adding or deleting the network node from the  
19 secure multicast or broadcast group; and

20 distributing the group session key from the first group controller to the other group  
21 controllers of the plurality of group controllers over the secure channel.

1 22. (Previously Presented) A method as recited in Claim 21, further comprising the step of  
2 generating the group session key only when the first group controller is designated as a  
3 master group controller that is authorized to join network nodes and generate group  
4 session keys.

1 23. (Previously Presented) A method as recited in Claim 22, further comprising the step of  
2 successively designating different group controllers of the plurality of group controllers  
3 as the master group controller in real time.

1 24. (Previously Presented) A method for creating a secure multicast or broadcast group, the  
2 method comprising the steps of:  
3 establishing a secure communication channel among a plurality of group controllers via a  
4 public key exchange protocol;  
5 load balancing traffic emanating from a plurality of network nodes to the plurality of  
6 group controllers; and  
7 distributing a group session key by one of the group controllers based upon a logical  
8 arrangement of the network nodes in a binary tree structure, the binary tree  
9 structure having a root node, intermediate nodes, and leaf nodes, wherein the  
10 plurality of network nodes correspond to leaf nodes of the binary tree structure  
11 and the plurality of group controllers correspond to the root node.

1 25. (Original) The method as recited in Claim 24, wherein the step of distributing further  
2 comprises:  
3 circulating a token among the plurality of group controllers to designate the one group  
4 controller as having permission to selectively generate the group session key and  
5 keys associated with the intermediate nodes and the leaf nodes; and  
6 selectively generating the group session key based upon the circulating step.

1 26. (Previously Presented) The method as recited in Claim 24, wherein the step of  
2 distributing further comprises:  
3 detecting whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the detecting  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key; and  
9 sending the new group session key to the leaf nodes.

1 27. (Previously Presented) The method as recited in Claim 26, wherein the step of updating  
2 comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.

1 28. (Previously Presented) The method as recited in Claim 24, wherein the step of  
2 distributing further comprises:  
3 receiving a request message from one of the plurality of network nodes to join the secure  
4 multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the receiving  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key and a private key of the joining node; and  
9 sending a message comprising the new group session key, the private key, and the  
10 updated keys of affected intermediate nodes to the joining node.

1 29. (Original) The method as recited in Claim 28, wherein the step of updating comprises  
2 performing a one way hash function on the keys associated with the affected intermediate  
3 nodes.



1 30. (Original) The method as recited in Claim 24, further comprising addressing the plurality  
2 of group controllers using a single virtual address.

1 31. (Previously Presented) A computer system that can manage addition and deletion of  
2 network nodes from and to a secure multicast or broadcast group of network nodes in a  
3 communications network without a single point of failure, wherein each of the network  
4 nodes is associated with one of a plurality of group controllers, wherein each group  
5 controller of the plurality of group controllers is a replica of a particular group controller,  
6 and wherein the network nodes and the plurality of group controllers are logically  
7 organized in a binary tree that represents the network nodes and the plurality of group  
8 controllers, in which leaf nodes of the binary tree represent network nodes that are  
9 joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
10 other network nodes, and root nodes represent the plurality of group controllers, the  
11 computer system comprising:  
12 a load balancer coupled to the plurality of group controllers for interfacing inbound service  
13 requests to a selected group controller of the plurality of group controllers;  
14 a bus coupled to the load balancer for transferring data;  
15 one or more processors coupled to the bus for selectively generating a group session key  
16 under control of program instructions;  
17 a memory coupled to the one or more processors via the bus;  
18 one or more sequences of program instructions stored in the memory which, when  
19 executed by the one or more processors cause the one or more processors to  
20 perform the steps of:  
21 joining a first group controller to the plurality of group controllers in a local network;  
22 establishing a secure communication channel between the first group controller and a  
23 second group controller of the plurality of group controllers using a key exchange  
24 protocol;  
25 receiving a request to add or delete a network node of the secure multicast or broadcast  
26 group from the load balancer that is coupled to the plurality of group controllers;

27 creating and storing a new group session key for each network node represented in each  
28 branch of the binary tree that is affected by adding or deleting the network node  
29 from the secure multicast or broadcast group;  
30 distributing the group session key from a third group controller of the plurality of group  
31 controllers to the network nodes.

1 32. (Previously Presented) A computer system as recited in Claim 31, wherein distributing a  
2 group session key further comprises:  
3 receiving a token value at the third group controller to designate the third group controller  
4 as having permission to selectively generate the group session key and to generate  
5 node keys associated with the intermediate nodes and the leaf nodes; and  
6 creating and storing the group session key only when the third group controller has the  
7 token value.

1 33. (Previously Presented) A computer system as recited in Claim 31, wherein distributing a  
2 group session key further comprises:  
3 determining whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected by the leaving node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key; and  
8 sending the new group session key to the leaf nodes.

1 34. (Previously Presented) A computer system as recited in Claim 33, wherein updating keys  
2 comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.

1 35. (Previously Presented) A computer system as recited in Claim 31, wherein distributing a  
2 group session key further comprises:

3 receiving a request message from one of the network nodes to join the secure multicast or  
4 broadcast group;  
5 determining which of the intermediate nodes are affected by the joining node;  
6 updating keys associated with the affected intermediate nodes;  
7 generating a new group session key and a private key of the joining node; and  
8 sending a message comprising the new group session key, the private key, and the  
9 updated keys of affected intermediate nodes to the joining node.

1 36. (Previously Presented) A computer system as recited in Claim 35, wherein updating keys  
2 comprises performing a one way hash function on the keys associated with the affected  
3 intermediate nodes.

1 37. (Previously Presented) A computer system as recited in Claim 31, wherein receiving a  
2 request comprises receiving the request at a load balancer having a single virtual address  
3 that represents the plurality of group controllers.

1 38. (Previously Presented) A computer system as recited in Claim 37, further comprising  
2 one or more sequences of program instructions stored in the memory which, when  
3 executed by the one or more processors cause the one or more processors to perform the  
4 step of load balancing network traffic that is directed from a plurality of the network  
5 nodes to the plurality of group controllers.

1 39. (Previously Presented) A computer system as recited in Claim 31, wherein establishing a  
2 secure communication channel comprises exchanging a public key of the first group  
3 controller with all other group controllers in the plurality of group controllers based upon  
4 optimized broadcast Diffie-Hellman protocol.

1 40. (Previously Presented) A computer system as recited in Claim 35, wherein establishing a  
2 secure communication channel comprises:  
3 receiving a public key value that is broadcast by the joining node;  
4 sending a collective public key value from the network nodes to the joining node;  
5 computing a shared secret key; and

6           creating and storing a group shared secret key by exchanging private key values.

1   41.   (Previously Presented) An apparatus for managing addition and deletion of network  
2       nodes from and to a secure multicast or broadcast group of network nodes in a  
3       communications network without a single point of failure, wherein each of the network  
4       nodes is associated with one of a plurality of group controllers, wherein each group  
5       controller of the plurality of group controllers is a replica of a particular group controller,  
6       and wherein the network nodes and the plurality of group controllers are logically  
7       organized in a binary tree that represents the network nodes and the plurality of group  
8       controllers, in which leaf nodes of the binary tree represent network nodes that are  
9       joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
10      other network nodes, and root nodes represent the plurality of group controllers, the  
11      apparatus comprising:  
12      means for joining a first group controller to the plurality of group controllers in a local  
13      network;  
14      means for establishing a secure communication channel between the first group controller  
15      and a second group controller of the plurality of group controllers using a key  
16      exchange protocol;  
17      means for receiving a request to add or delete a network node of the secure multicast or  
18      broadcast group from a load balancer that is coupled to the plurality of group  
19      controllers;  
20      means for creating and storing a new group session key for each network node  
21      represented in each branch of the binary tree that is affected by adding or deleting  
22      the network node from the secure multicast or broadcast group; and  
23      means for distributing a group session key from a third group controller of the plurality of  
24      group controllers to the network nodes.

1   42.   (Previously Presented) An apparatus as recited in Claim 41, wherein the means for  
2       distributing a group session key further comprises:

3 means for receiving a token value at the third group controller to designate the third  
4 group controller as having permission to selectively generate the group session  
5 key and to generate node keys associated with the intermediate nodes and the leaf  
6 nodes; and  
7 means for creating and storing the group session key only when the third group controller  
8 has the token value.

1 43. (Previously Presented) An apparatus as recited in Claim 41, wherein the means for  
2 distributing a group session key further comprises:  
3 means for determining whether the secure multicast or broadcast group has a network  
4 node that is leaving the secure multicast or broadcast group;  
5 means for determining which of the intermediate nodes are affected by the leaving node;  
6 means for updating keys associated with the affected intermediate nodes;  
7 means for generating a new group session key; and  
8 means for sending the new group session key to the leaf nodes.

1 44. (Previously Presented) An apparatus as recited in Claim 43, wherein the means for  
2 updating keys comprises:  
3 means for generating a new key of a parent node of the leaving node; and  
4 means for encrypting the new key of the parent node with a key of a network node  
5 adjacent to the parent node.

1 45. (Previously Presented) An apparatus as recited in Claim 41, wherein the means for  
2 distributing a group session key further comprises:  
3 means for receiving a request message from one of the network nodes to join the secure  
4 multicast or broadcast group;  
5 means for determining which of the intermediate nodes are affected by the joining node;  
6 means for updating keys associated with the affected intermediate nodes;  
7 means for generating a new group session key and a private key of the joining node; and  
8 means for sending a message comprising the new group session key, the private key, and  
9 the updated keys of affected intermediate nodes to the joining node.

- 1 46. (Previously Presented) An apparatus as recited in Claim 45, wherein the means for  
2 updating keys comprises means for performing a one way hash function on the keys  
3 associated with the affected intermediate nodes.
- 1 47. (Previously Presented) An apparatus as recited in Claim 41, wherein the means for  
2 receiving a request comprises means for receiving the request at a load balancer having a  
3 single virtual address that represents the plurality of group controllers.
- 1 48. (Previously Presented) An apparatus as recited in Claim 47, further comprising means  
2 for load balancing network traffic that is directed from a plurality of the network nodes to  
3 the plurality of group controllers.
- 1 49. (Previously Presented) An apparatus as recited in Claim 41, wherein the means for  
2 establishing a secure communication channel comprises means for exchanging a public  
3 key of the first group controller with all other group controllers in the plurality of group  
4 controllers based upon optimized broadcast Diffie-Hellman protocol.
- 1 50. (Previously Presented) An apparatus as recited in Claim 45, wherein the means for  
2 establishing a secure communication channel comprises:  
3 means for receiving a public key value that is broadcast by the joining node;  
4 means for sending a collective public key value from the network nodes to the joining  
5 node;  
6 means for computing a shared secret key; and  
7 means for creating and storing a group shared secret key by exchanging private key  
8 values.
- 1 51. (Currently Amended) A computer-readable storage medium comprising one or more  
2 sequences of executable instructions for managing addition and deletion of network  
3 nodes from and to a secure multicast or broadcast group of network nodes in a  
4 communications network, wherein each of the network nodes is associated with a first  
5 group controller comprising information that is replicated in a plurality of group

6 controllers, and wherein the network nodes and the plurality of group controllers are  
7 logically organized in a binary tree that represents the network nodes and the plurality of  
8 group controllers, in which leaf nodes of the binary tree represent network nodes that are  
9 joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
10 other network nodes, and root nodes represent the plurality of group controllers, and  
11 which instructions, when executed by one or more processors, cause the processors to  
12 carry out the steps of:  
13 joining the first group controller in a local network in which the plurality of group  
14 controllers are coupled;  
15 establishing a secure channel between the first group controller and the plurality of group  
16 controllers through secure key exchange;  
17 receiving a request to add or delete a network node from a load balancer that controls  
18 distribution of requests to the plurality of group controllers;  
19 generating a new group session key for each network node represented in each branch of  
20 the binary tree that is affected by adding or deleting the network node from the  
21 secure multicast or broadcast group; and  
22 distributing the group session key from the first group controller to the other group  
23 controllers of the plurality of group controllers over the secure channel.

1 52. (Currently Amended) A computer-readable storage medium as recited in Claim 51,  
2 further comprising executable instructions to carry out the step of generating the group  
3 session key only when the first group controller is designated as a master group  
4 controller that is authorized to join network nodes and generate group session keys.

1 53. (Currently Amended) A computer-readable storage medium as recited in Claim 52,  
2 further comprising executable instructions for carrying out the step of successively  
3 designating different group controllers of the plurality of group controllers as the master  
4 group controller in real time.

1 54. (Currently Amended) A computer-readable storage medium comprising one or more  
2 sequences of executable instructions for creating a secure multicast or broadcast group,

3 and which instructions, when executed by one or more processors, cause the processors  
4 to carry out the steps of:  
5 establishing a secure communication channel among a plurality of group controllers via a  
6 public key exchange protocol;  
7 load balancing traffic emanating from a plurality of network nodes to the plurality of  
8 group controllers; and  
9 distributing a group session key by one of the group controllers based upon a logical  
10 arrangement of the network nodes in a binary tree structure, the binary tree  
11 structure having a root node, intermediate nodes, and leaf nodes, wherein the  
12 plurality of network nodes correspond to leaf nodes of the binary tree structure  
13 and the plurality of group controllers correspond to the root node.

1 55. (Currently Amended) The computer-readable storage medium as recited in Claim 54,  
2 wherein the step of distributing further comprises:  
3 circulating a token among the plurality of group controllers to designate the one group  
4 controller as having permission to selectively generate the group session key and  
5 keys associated with the intermediate nodes and the leaf nodes; and  
6 selectively generating the group session key based upon the circulating step.

1 56. (Currently Amended) The computer-readable storage medium as recited in Claim 54,  
2 wherein the step of distributing further comprises:  
3 detecting whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the detecting  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key; and  
9 sending the new group session key to the leaf nodes.



1 57. (Currently Amended) The computer-readable storage medium as recited in Claim 56,  
2 wherein the step of updating comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.

1 58. (Currently Amended) The computer-readable storage medium as recited in Claim 54,  
2 wherein the step of distributing further comprises:  
3 receiving a request message from one of the plurality of network nodes to join the secure  
4 multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the receiving  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key and a private key of the joining node; and  
9 sending a message comprising the new group session key, the private key, and the  
10 updated keys of affected intermediate nodes to the joining node.

1 59. (Currently Amended) The computer-readable storage medium as recited in Claim 58,  
2 wherein the step of updating comprises performing a one way hash function on the keys  
3 associated with the affected intermediate nodes.

1 60. (Currently Amended) The computer-readable storage medium as recited in Claim 54,  
2 further comprising instructions for carrying out the step of addressing the plurality of  
3 group controllers using a single virtual address.

1 61. (Previously Presented) A computer system that can manage addition and deletion of  
2 network nodes from and to a secure multicast or broadcast group of network nodes in a  
3 communications network, wherein each of the network nodes is associated with a first  
4 group controller comprising information that is replicated in a plurality of group  
5 controllers, and wherein the network nodes and the plurality of group controllers are  
6 logically organized in a binary tree that represents the network nodes and the plurality of

7 group controllers, in which leaf nodes of the binary tree represent network nodes that are  
8 joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
9 other network nodes, and root nodes represent the plurality of group controllers, the  
10 computer system comprising:  
11 a load balancer coupled to the plurality of group controllers for interfacing inbound  
12 service requests to a selected group controller of the plurality of group controllers;  
13 a bus coupled to the load balancer for transferring data;  
14 one or more processors coupled to the bus for selectively generating a group session key  
15 under control of program instructions;  
16 a memory coupled to the one or more processors via the bus;  
17 one or more sequences of program instructions stored in the memory which, when  
18 executed by the one or more processors cause the one or more processors to  
19 perform the steps of:  
20 joining the first group controller in a local network in which the plurality of group  
21 controllers are coupled;  
22 establishing a secure channel between the first group controller and the plurality of group  
23 controllers through secure key exchange;  
24 receiving a request to add or delete a network node from the load balancer that controls  
25 distribution of requests to the plurality of group controllers;  
26 generating a new group session key for each network node represented in each branch of  
27 the binary tree that is affected by adding or deleting the network node from the  
28 secure multicast or broadcast group; and  
29 distributing the group session key from the first group controller to the other group  
30 controllers of the plurality of group controllers over the secure channel.

- 1 62. (Previously Presented) A computer system as recited in Claim 61, further comprising  
2 instructions to perform the step of generating the group session key only when the first  
3 group controller is designated as a master group controller that is authorized to join  
4 network nodes and generate group session keys.

1 63. (Previously Presented) A computer system as recited in Claim 62, further comprising  
2 instructions to perform the step of successively designating different group controllers of  
3 the plurality of group controllers as the master group controller in real time.

1 64. (Previously Presented) A computer system that can create a secure multicast or broadcast  
2 group, the computer system comprising:  
3 a load balancer coupled to the plurality of group controllers for interfacing inbound  
4 service requests to a selected group controller of the plurality of group controllers;  
5 a bus coupled to the load balancer for transferring data;  
6 one or more processors coupled to the bus for selectively generating a group session key  
7 under control of program instructions;  
8 a memory coupled to the one or more processors via the bus;  
9 one or more sequences of program instructions stored in the memory which, when  
10 executed by the one or more processors cause the one or more processors to  
11 perform the steps of:  
12 establishing a secure communication channel among a plurality of group controllers via a  
13 public key exchange protocol;  
14 load balancing traffic emanating from a plurality of network nodes to the plurality of  
15 group controllers; and  
16 distributing a group session key by one of the group controllers based upon a logical  
17 arrangement of the network nodes in a binary tree structure, the binary tree  
18 structure having a root node, intermediate nodes, and leaf nodes, wherein the  
19 plurality of network nodes correspond to leaf nodes of the binary tree structure  
20 and the plurality of group controllers correspond to the root node.

1 65. (Previously Presented) The computer system as recited in Claim 64, wherein the step of  
2 distributing further comprises:  
3 circulating a token among the plurality of group controllers to designate the one group  
4 controller as having permission to selectively generate the group session key and  
5 keys associated with the intermediate nodes and the leaf nodes; and

6 selectively generating the group session key based upon the circulating step.

1 66. (Previously Presented) The computer system as recited in Claim 64, wherein the step of  
2 distributing further comprises:  
3 detecting whether the secure multicast or broadcast group has a network node that is  
4 leaving the secure multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the detecting  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key; and  
9 sending the new group session key to the leaf nodes.

1 67. (Previously Presented) The computer system as recited in Claim 66, wherein the step of  
2 updating comprises:  
3 generating a new key of a parent node of the leaving node; and  
4 encrypting the new key of the parent node with a key of a network node adjacent to the  
5 parent node.

1 68. (Previously Presented) The computer system as recited in Claim 64, wherein the step of  
2 distributing further comprises:  
3 receiving a request message from one of the plurality of network nodes to join the secure  
4 multicast or broadcast group;  
5 determining which of the intermediate nodes are affected in response to the receiving  
6 step;  
7 updating keys associated with the affected intermediate nodes;  
8 generating a new group session key and a private key of the joining node; and  
9 sending a message comprising the new group session key, the private key, and the  
10 updated keys of affected intermediate nodes to the joining node.

1 69. (Previously Presented) The computer system as recited in Claim 68, wherein the step of  
2 updating comprises performing a one way hash function on the keys associated with the  
3 affected intermediate nodes.

1 70. (Previously Presented) The computer system as recited in Claim 64, further comprising  
2 instructions to perform the step of addressing the plurality of group controllers using a  
3 single virtual address.

1 71. (Previously Presented) An apparatus for managing addition and deletion of network  
2 nodes from and to a secure multicast or broadcast group of network nodes in a  
3 communications network, wherein each of the network nodes is associated with a first  
4 group controller comprising information that is replicated in a plurality of group  
5 controllers, and wherein the network nodes and the plurality of group controllers are  
6 logically organized in a binary tree that represents the network nodes and the plurality of  
7 group controllers, in which leaf nodes of the binary tree represent network nodes that are  
8 joining or leaving the secure multicast or broadcast group, intermediate nodes represent  
9 other network nodes, and root nodes represent the plurality of group controllers, the  
10 apparatus comprising:  
11 means for joining the first group controller in a local network in which the plurality of  
12 group controllers are coupled;  
13 means for establishing a secure channel between the first group controller and the  
14 plurality of group controllers through secure key exchange;  
15 means for receiving a request to add or delete a network node from a load balancer that  
16 controls distribution of requests to the plurality of group controllers;  
17 means for generating a new group session key for each network node represented in each  
18 branch of the binary tree that is affected by adding or deleting the network node  
19 from the secure multicast or broadcast group; and  
20 means for distributing the group session key from the first group controller to the other  
21 group controllers of the plurality of group controllers over the secure channel.

1 72. (Previously Presented) An apparatus as recited in Claim 71, further comprising means  
2 for generating the group session key only when the first group controller is designated as  
3 a master group controller that is authorized to join network nodes and generate group  
4 session keys.

1 73. (Previously Presented) An apparatus as recited in Claim 72, further comprising means  
2 for successively designating different group controllers of the plurality of group  
3 controllers as the master group controller in real time.

1 74. (Previously Presented) An apparatus for creating a secure multicast or broadcast group,  
2 the apparatus comprising:  
3 means for establishing a secure communication channel among a plurality of group  
4 controllers via a public key exchange protocol;  
5 means for load balancing traffic emanating from a plurality of network nodes to the  
6 plurality of group controllers; and  
7 means for distributing a group session key by one of the group controllers based upon a  
8 logical arrangement of the network nodes in a binary tree structure, the binary tree  
9 structure having a root node, intermediate nodes, and leaf nodes, wherein the  
10 plurality of network nodes correspond to leaf nodes of the binary tree structure  
11 and the plurality of group controllers correspond to the root node.

1 75. (Previously Presented) The apparatus as recited in Claim 74, wherein the means for  
2 distributing further comprises:  
3 means for circulating a token among the plurality of group controllers to designate the  
4 one group controller as having permission to selectively generate the group  
5 session key and keys associated with the intermediate nodes and the leaf nodes;  
6 and  
7 means for selectively generating the group session key based upon the circulating step.

1 76. (Previously Presented) The apparatus as recited in Claim 74, wherein the means for  
2 distributing further comprises:  
3 means for detecting whether the secure multicast or broadcast group has a network node  
4 that is leaving the secure multicast or broadcast group;  
5 means for determining which of the intermediate nodes are affected in response to the  
6 detecting means;

- 7 means for updating keys associated with the affected intermediate nodes;
- 8 means for generating a new group session key; and
- 9 means for sending the new group session key to the leaf nodes.

1 77. (Previously Presented) The apparatus as recited in Claim 76, wherein the means for  
2 updating comprises:

- 3 means for generating a new key of a parent node of the leaving node; and
- 4 means for encrypting the new key of the parent node with a key of a network node
- 5 adjacent to the parent node.

1 78. (Previously Presented) The apparatus as recited in Claim 74, wherein the means for  
2 distributing further comprises:

- 3 means for receiving a request message from one of the plurality of network nodes to join
- 4 the secure multicast or broadcast group;
- 5 means for determining which of the intermediate nodes are affected in response to the
- 6 receiving means;
- 7 means for updating keys associated with the affected intermediate nodes;
- 8 means for generating a new group session key and a private key of the joining node; and
- 9 means for sending a message comprising the new group session key, the private key, and
- 10 the updated keys of affected intermediate nodes to the joining node.

1 79. (Previously Presented) The apparatus as recited in Claim 78, wherein the means for  
2 updating comprises means for performing a one way hash function on the keys associated  
3 with the affected intermediate nodes.

1 80. (Previously Presented) The apparatus as recited in Claim 74, further comprising means  
2 for addressing the plurality of group controllers using a single virtual address.